

Hacking Articles

Raj Chandel's Blog



Menu

[Home](#) » [Footprinting](#) » [Beginner Guide to Website Footprinting](#)

Footprinting

Beginner Guide to Website Footprinting

July 23, 2017 By Raj Chandel

In our **previous** article, we have discussed a brief introduction of footprinting for gathering information related to the specific person. As we had discussed that there are so many types of footprinting and today we are going to talk about DNS footprinting, website footprinting, and whois footprinting.

Browsing the target Website may Providing

- Whos is Details
- Software used and version
- OS Details
- Sub Domains
- File Name and File Path
- Scripting Platform & CMS Details
- Contact Details

Let's start!!

From Wikipedia

Whois footprinting

WHOIS (pronounced as the phrase who is) is a query and response protocol and whois footprinting is a method for glance information about ownership of a domain name as following:

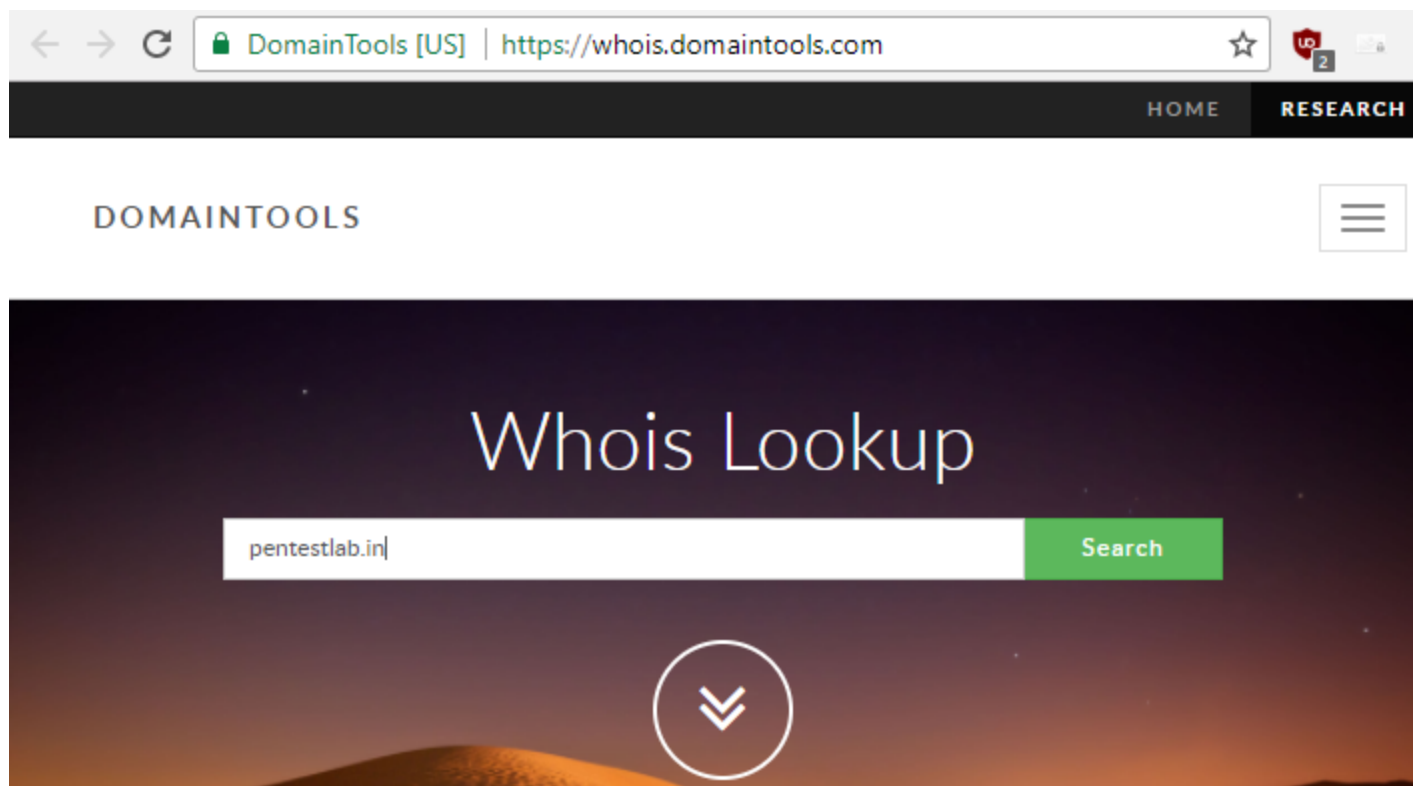
- Domain name details
- Contact details contain phone no. and email address of the owner
- Registration date for the domain name
- Expire date for the domain name
- Domain name servers

Whois Lookup

It is broadly used in support of querying databases that store the registered users or assignees of an Internet resource, such as **a domain name, an IP address block, or an autonomous system**, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

Browse given URL **<http://whois.domaintools.com/>** in browser and type any domain name.

For example: let's search **pentestlab.in**



Now you can see it has created a whois record for pentestlab.in where it contains details like **email address, IP, registrant Org**. From the given record, anyone can guess that this domain has some connection to raj chandel. The attacker needs to perform footprinting on raj chandel taking help from the previous article.

There is so many other tools use for whois footprinting for example:

- **Caller IP**
- **Whois Analyzer pro**
- **Whois lookup multiple addresses**

Whois Record for PentestLab.in

— Whois & Quick Stats

Email	rrajchandel@gmail.com is associated with ~8 domains	↻
Registrant Org	RAJ Chandel is associated with ~2 other domains	↻
Dates	Created on 2017-07-11 - Expires on 2018-07-11 - Updated on 2017-07-11	↻
IP Address	72.52.229.111 - 120 other sites hosted on this server	↻
IP Location	🇺🇸 - Michigan - Lansing - Liquid Web L.L.c	
ASN	🇺🇸 AS32244 LIQUID-WEB-INC - Liquid Web, L.L.C, US (registered Mar 26, 2004)	
Whois History	3 records have been archived since 2017-07-11	↻
Whois Server	whois.inregistry.net	

— Website

Website Title	🌐 Ignite lab	↻
---------------	--------------	---

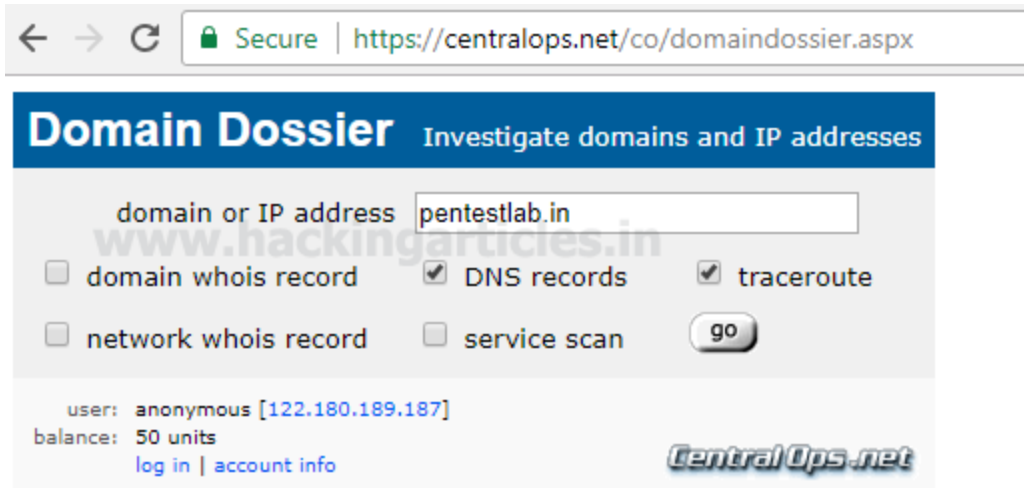
DNS Footprinting

The attacker performs DNS footprinting in order to enumerate DNS record details and type of servers. There is 10 type of DNS record which provide important information related to the target location.

1. A/AAAA
2. SVR
3. NS
4. TXT
5. MX
6. CNAME
7. SOA
8. RP
9. PTR
10. HINFO

Domain Dossier: it is an online tool use for complete DNS footprinting as well as whois footprinting.

There are so many online tool use for DNS footprinting, using domain dossier we will check for DNS records of penetstlab.in, select the check box for **DNS records** and traceroute and then click on **go**.



Domain Dossier Investigate domains and IP addresses

domain or IP address

☐ domain whois record ☒ DNS records ☒ traceroute

☐ network whois record ☐ service scan

user: anonymous [122.180.189.187]
balance: 50 units
[log in](#) | [account info](#)

CentralOps.net

You can observe that the data which we received from whois lookup and from domain dossier is the same to some extent. It has given same email ID as above i.e. **rrajchandel@gmail.com** and moreover details of DNS records TXT, SOA, NS, MX, A and PTR.

DNS records

name	class	type	data	time to live
pentestlab.in	IN	TXT	v=spf1 +a +mx +ip4:72.52.218.232 ~all	14400s (04:00:00)
pentestlab.in	IN	SOA	server: dns1.rightdns.com email: rrajchandel@gmail.com serial: 2017071105 refresh: 3600 retry: 7200 expire: 1209600 minimum ttl: 86400	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns2.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns11.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns1.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns12.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	A	72.52.229.111	14400s (04:00:00)
pentestlab.in	IN	MX	preference: 0 exchange: pentestlab.in	14400s (04:00:00)
111.229.52.72.in-addr.arpa	IN	PTR	sun.rightdns.com	3600s (01:00:00)
229.52.72.in-addr.arpa	IN	NS	ns1.sourcedns.com	300s (00:05:00)

DNS Dumpster: it is also an online use for DNS footprinting.

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Enumerate a domain and pull back up to 40K subdomains, results are available in an XLS for easy reference.

Repeating the same process for **pentestlab.in**, it will search for its DNS record. From the given screenshot, you can observe we have received the same details as above. More it will create a copy as an output file in from XLS.

DNS Servers		
dns2.rightdns.com. 	72.52.205.50 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States
dns11.rightdns.com. 	72.52.204.44 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States
dns12.rightdns.com. 	72.52.205.50 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States
dns1.rightdns.com. 	72.52.204.44 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States
MX Records ** This is where email for the domain goes...		
0 pentestlab.in. 	72.52.229.111 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"v=spf1 +a +mx +ip4:72.52.218.232 ~all"		
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
pentestlab.in 	72.52.229.111 sun.rightdns.com	AS32244 Liquid Web, L.L.C United States

You get signal: it is also an online tool used for DNS footprinting as well as for Network footprinting

A **reverse IP domain check** takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete

Hence we get the **IP 72.52.229.111** for **pentestlab.in** moreover it dumped the name of **14** other domain which is hosted on the same web server.



Website Footprinting

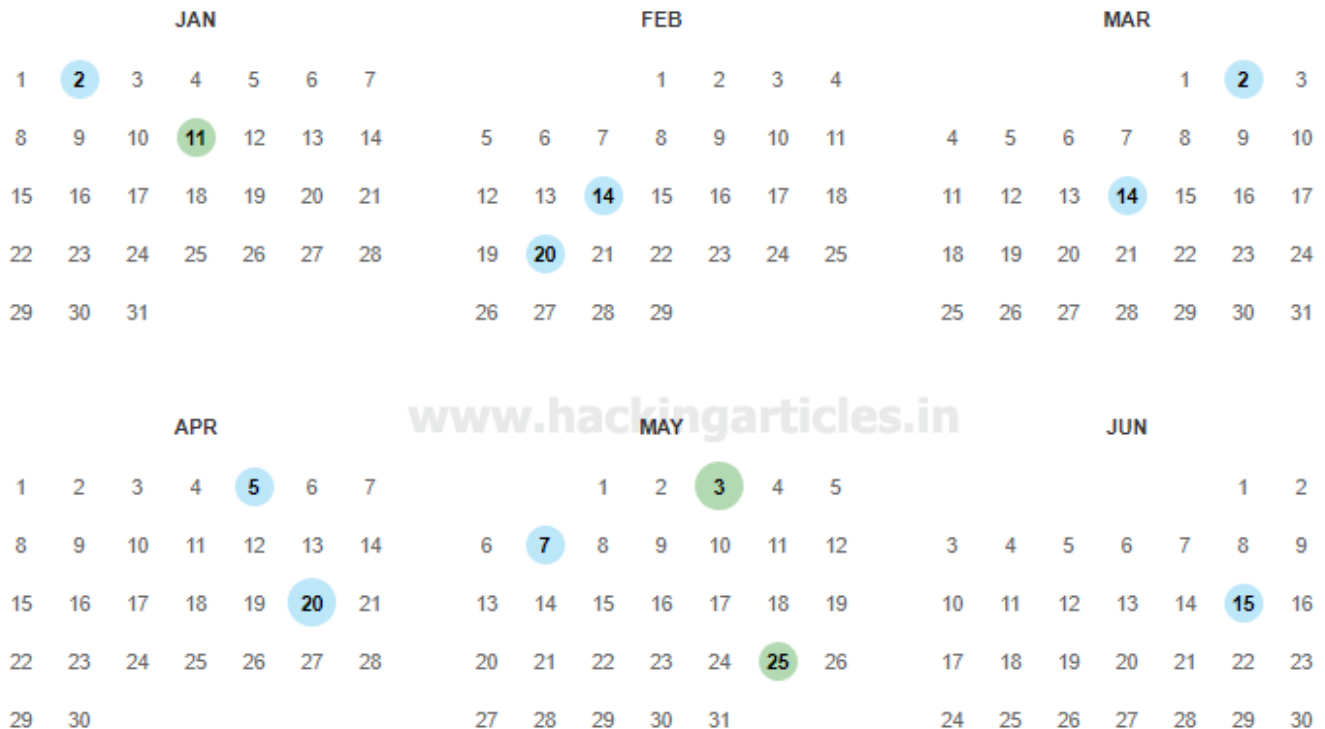
It is a technique used for extracting the details related to the website as following

1. Archived description of the website
2. Content management system and framework
3. Script and platform of the website and web server
4. Web crawling
5. Extract metadata and contact details from the website
6. Website and web page monitoring and analyzer

Archive.org: It is an online tool use for visiting the **archived version** of any website.

Archive.org has search option as **way back machine** which is like a time machine for any website. It contains entire information from past till present scenario of any website either their layout or content everything related to the website is present inside. In simple words, it contains the history of any website.

For example, I had a search for the **hackingarticles.in** the archived record of **2012**.



Built With: It is an online tool used for detecting techniques and framework involved inside running website.

BuiltWith.com technology tracking includes widgets, analytics, frameworks, content management systems, advertisers, content delivery networks, web standards, and web servers to name some of the technology categories.

Taking the example of hackingarticles.in again we found the following things:

- Content Management system: **WordPress**
- Framework: **PHP**

[BuiltWith Pty Ltd \[AU\]](#) | <https://builtwith.com/hackingarticles.in>

Log In · Sign Up for Free

 Tools ▾ Features ▾ Plans & Pricing Customers Resources ▾

Content Management Systems [View Global Trends](#)

 **WordPress**
[WordPress Usage Statistics - Download list of all WordPress websites](#) ⓘ
WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability.

 **WordPress Weekly Activity**
[WordPress Weekly Activity Usage Statistics - Download list of all WordPress Weekly Activity websites](#) ⓘ

 **Wordpress 4.7**
[Wordpress 4.7 Usage Statistics - Download list of all Wordpress 4.7 websites](#) ⓘ

 **Wordpress 4.8**
[Wordpress 4.8 Usage Statistics - Download list of all Wordpress 4.8 websites](#) ⓘ

Frameworks [View Global Trends](#)

 **PHP**
[PHP Usage Statistics - Download list of all PHP websites](#) ⓘ
PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

Advertising [View Global Trends](#)

 **eXelate**

Whatweb

Whatweb can identify all sorts of information about a live website, like Platform, CMS platform, Type of Script, Google Analytics, Web server Platform, and IP address Country. A pentester can use this tool as both a recon tool & vulnerability scanner.

Open the terminal in Kali Linux and type following command

```
whatweb www.pentestlab.in
```

As result, we receive the same information as above

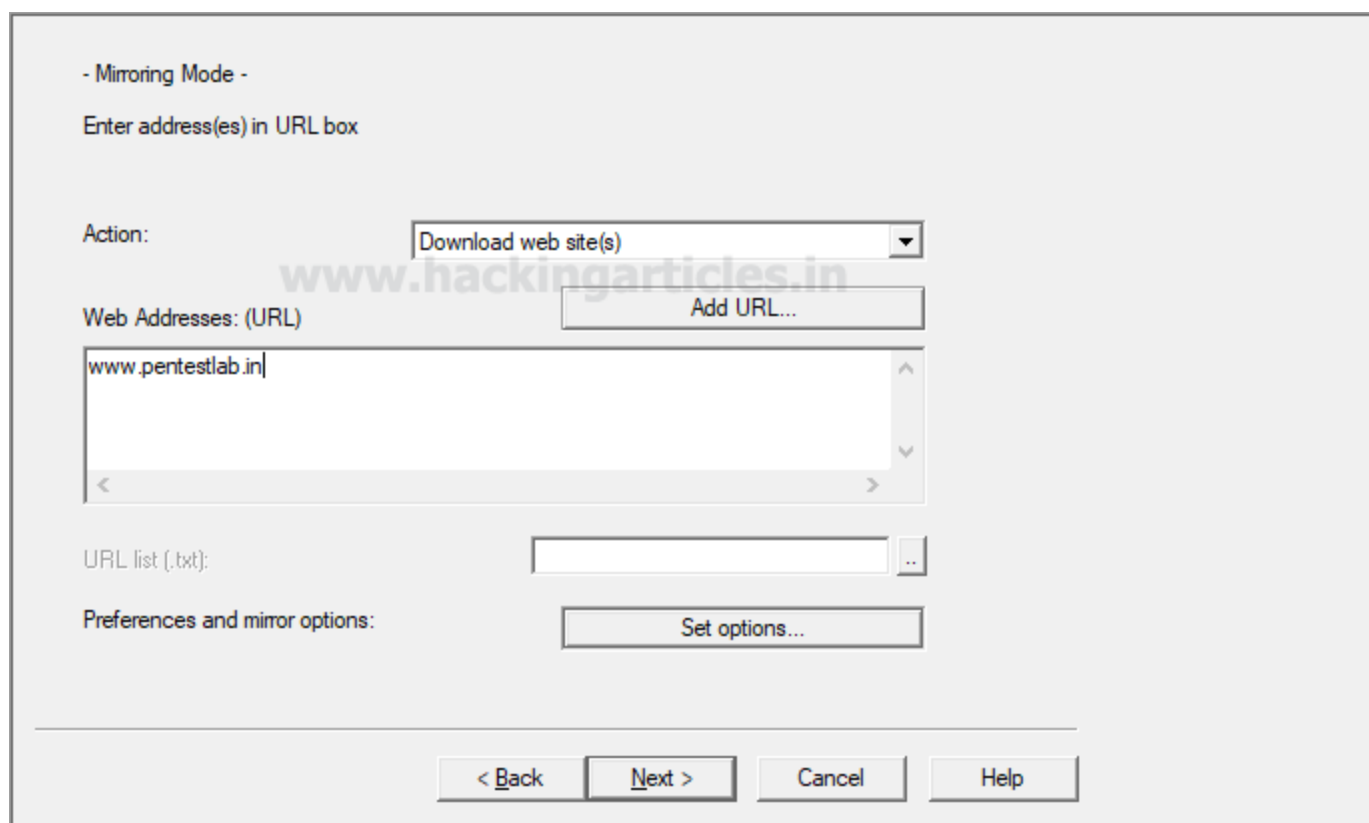
```
root@kali:~# whatweb www.pentestlab.in
http://www.pentestlab.in [200 OK] Apache, Country[UNITED STATES][US], HTML5, HTTPServer[Apache], IP[72.52.229.111], JQuery, Script, Title[Ignite lab]
```

Web crawling

HTTrack is a free and open source Web crawler and offline browser, developed by Xavier Roche

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure.

Give target URL for copy the web site as www.pentestlab.in which starts downloading the website.



<http://www.hackingarticles.in/5-ways-crawl-website/>

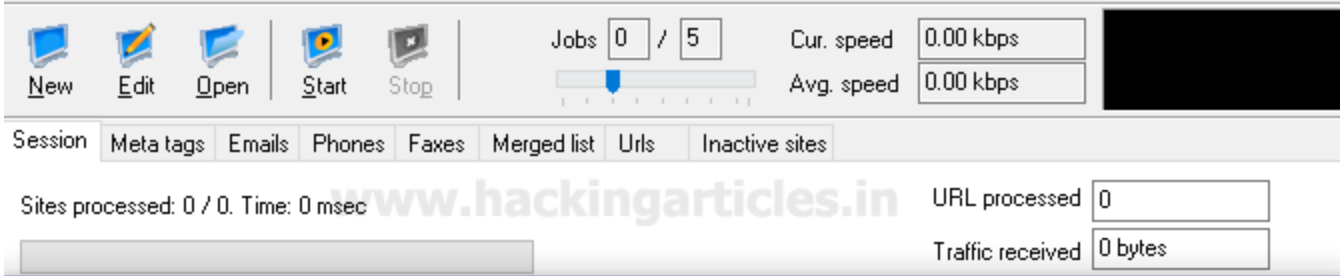
Web Data Extractor

Web Data Extractor Pro is a web scraping tool specifically designed for mass-gathering of various data types. It can **harvest URLs, phone and fax numbers, email addresses**, as well as meta tag information and body text. A special feature of WDE Pro is custom extraction of structured data.

Start new project Type target URL as ignitetechnologies.in and select folder to save the output and click on **ok**.

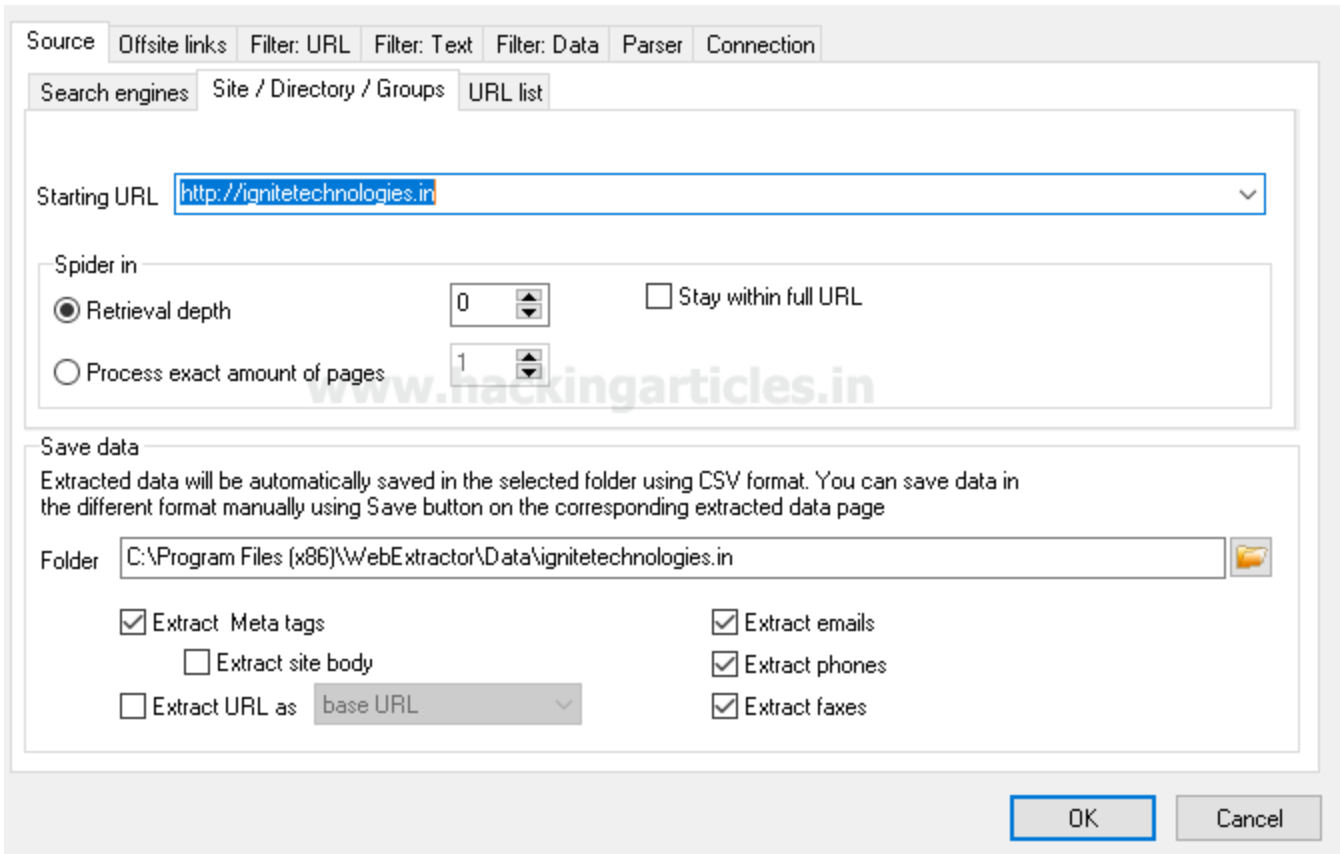
 Web Data Extractor 8.3

File View Help



The main interface of Web Data Extractor 8.3. It features a menu bar (File, View, Help) and a toolbar with icons for New, Edit, Open, Start, and Stop. A status bar at the top shows 'Jobs 0 / 5', 'Cur. speed 0.00 kbps', and 'Avg. speed 0.00 kbps'. Below the toolbar is a tabbed interface with 'Session' selected. The 'Session' tab shows 'Sites processed: 0 / 0. Time: 0 msec' and a progress bar. On the right, there are input fields for 'URL processed' (0) and 'Traffic received' (0 bytes).

Session settings



The 'Session settings' dialog box. It has tabs for 'Source', 'Offsite links', 'Filter: URL', 'Filter: Text', 'Filter: Data', 'Parser', and 'Connection'. The 'Source' tab is active, showing 'Search engines', 'Site / Directory / Groups', and 'URL list'. The 'Starting URL' is set to 'http://ignitetechnologies.in'. Under 'Spider in', 'Retrieval depth' is set to 0, and 'Stay within full URL' is unchecked. 'Process exact amount of pages' is set to 1. The 'Save data' section explains that data is saved in CSV format. The 'Folder' is 'C:\Program Files (x86)\WebExtractor\Data\ignitetechnologies.in'. Checkboxes for 'Extract Meta tags', 'Extract emails', 'Extract site body', 'Extract phones', 'Extract URL as' (set to 'base URL'), and 'Extract faxes' are all checked. 'OK' and 'Cancel' buttons are at the bottom right.

Now, this tool will extract metadata, email contact no. and etc from inside the target URL.

From given screenshot, you can see it found **40 meta tags** **1 email** **84-phone number** from ignitetechnologies.in website.

Similarly the other tool use as web data extractor:

Web spider

Web Data Extractor 8.3

File View Help

New Edit Open Start Stop

Jobs 0 / 5 Cur. speed 0.00 kbps Avg. speed 1.19 kbps

Session Meta tags (40) Emails (1) Phones (84) Faxes (84) Merged list Urls Inactive sites

www.hackingarticles.in

Phone	Source	Tag	URL	Title
01145103130	011 - 45103130		http://ignitetechnologies.in/junior.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/Licensed-Penetration-	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/Licensed-Penetration-	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/malware.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/malware.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/MCSA.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/MCSA.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/MCSE.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/MCSE.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/media-section.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/media-section.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/Networking-Training.p	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/Networking-Training.p	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/online_training.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/online_training.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/PHP-Training.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/PHP-Training.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
9101145103130	+91-011-45103130	Call	http://ignitetechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91-9599387841		http://ignitetechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitetechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitetechnologies.in/RHCE.php	Ethical Hacking Training Institute Certified Ethic.

Competitive Intelligence

Website-Watcher is a **powerful yet simple website-monitoring tool**, perfectly suited to the beginner and advanced user alike. You can download it from **here**.

Using **the new** tab and enter the target URL which starts monitoring the target website.

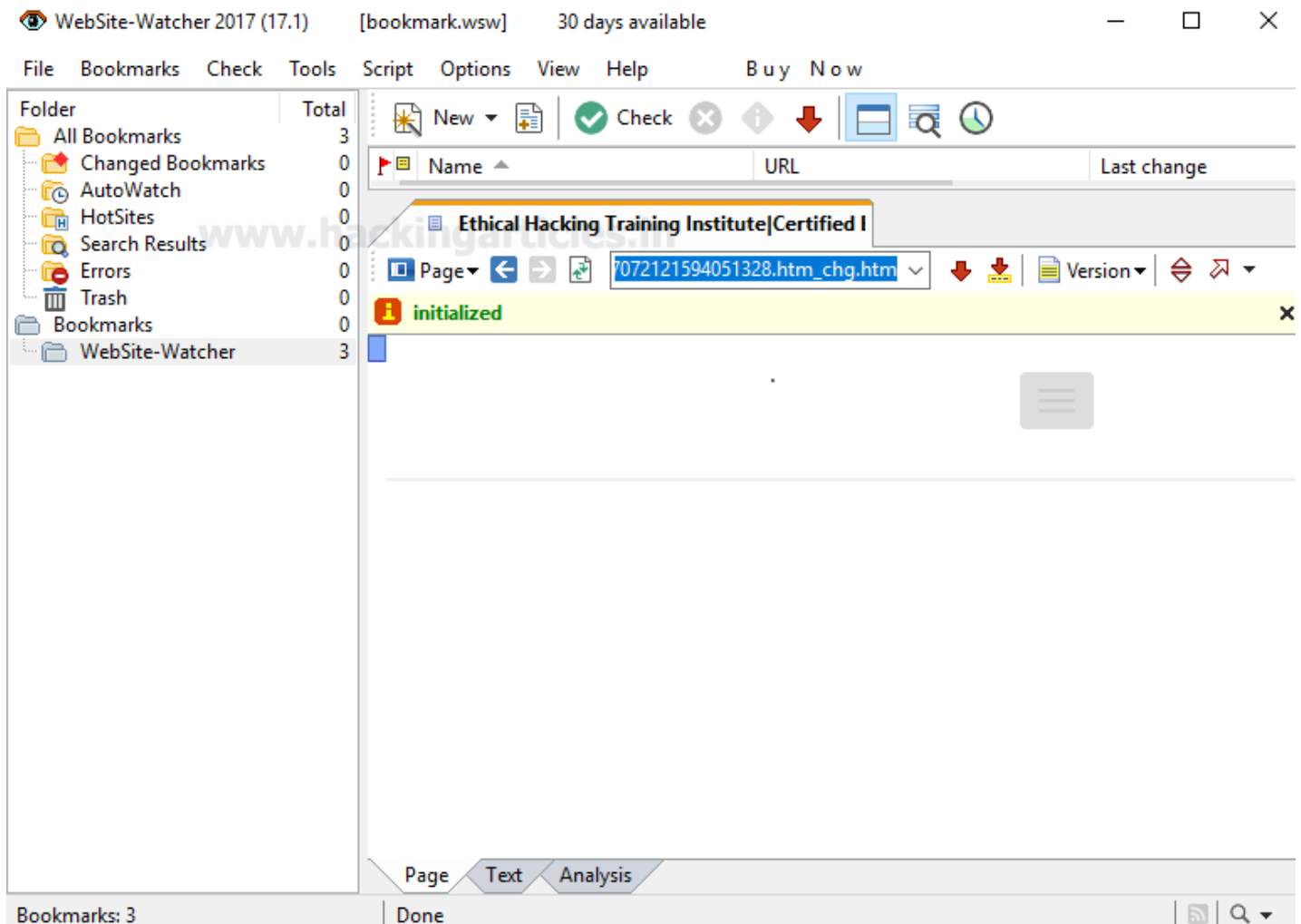
For example, I enter the URL hackingarticles.in for monitoring this website.

Similarly, there are some other tools uses for monitoring:

On web change

Follow that page

Informinder



Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

◀ PREVIOUS POST

3 ways to scan Eternal Blue Vulnerability in Remote PC

NEXT POST ▶

Hack the d0not5top VM (CTF Challenge)

Join Our Training Program





Categories

Cryptography & Steganography

CTF Challenges

Cyber Forensics

Database Hacking

Footprinting

Hacking Tools

Kali Linux

Nmap

Others

Password Cracking

Penetration Testing

Pentest Lab Setup

Privilege Escalation

Red Teaming

Social Engineering Toolkit

Uncategorized

Website Hacking

Window Password Hacking

Wireless Hacking

Wireless Penetration Testing

Archives

Select Month



You may like

Beginner Guide to Footprinting

June 20, 2017

6 ways to Find Connected PC in your Network (Beginner Guide)

January 3, 2016